CLAIMS

1. A digital certification method, comprising the steps of:

storing, at a first time, a first signature dependent upon a first user identity and a first user system in combination;

generating, at a second time subsequent to said first time, a second signature dependent upon a second user identity and a second user system in combination; and

certifying, in dependence upon said first and second signatures, whether the combination of said second user identity and said second user system match the combination of said first user identity and said first user system.

2. A method according to claim 1, wherein said step of storing comprises the step of developing said first signature in dependence upon a first user identity code and in dependence further upon a first group of at least one component as present in said first user system at said first time.

3. A method according to claim 2, wherein said step of developing said first signature comprises the

step of obtaining said first user identity code in response to user input.

4. A method according to claim 2, wherein said step of storing further comprises the step of storing said first signature accessibly to a certification server,

and wherein said step of certifying comprises the step of said certification server developing a certification result in dependence upon said first and second signatures.

5. A method according to claim 1, wherein said second user system is said first user system.

6. A method according to claim 1, wherein said step of certifying comprises the step of certifying, in dependence upon said first and second signatures, whether the combination of said second user identity and said second user system match the combination of said first user identity and said first user system, and further that said second signature was generated at a time different from said first time.

7. A method according to claim 6, wherein said step of generating is performed in response to a

challenge, wherein said second signature is further dependent upon said challenge, and wherein said step of certifying comprises the step of developing a certification result in dependence upon said first and second signatures and further in dependence upon said challenge.

8. A method according to claim 1, further comprising the step of providing a challenge code,

wherein said second signature is further dependent upon said challenge code.

9. A method according to claim 8, wherein said step of certifying comprises the step of developing a certification result in dependence upon said first and second signatures and further in dependence upon said challenge code.

10. A method according to claim 9, wherein said step of storing a first signature comprises the step of storing said first signature accessibly to a certification server,

wherein said step of providing a challenge code comprises the step of an inquiring system providing said challenge code to both said second user system and said certification server,

wherein said step of generating a second signature comprises the step of said second user system generating said second signature, said second signature being provided to said certification server,

and wherein said step of developing a certification result is performed by said certification server.

11. A method according to claim 10, wherein said step of certifying further comprises the step of providing said certification result to said inquiring system.

12. A method according to claim 1, wherein said step of storing a first signature comprises the step of storing said first signature accessibly to a certification server, and wherein said first user system comprises a first group of components, comprising the steps of:

developing a first component signature of each respective component in said first group as present in said first user system at said first time; and

storing said first component signatures accessibly to said certification server.

13. A method according to claim 12, wherein said second user system comprises a second group of components, wherein said first signature is different from said first component signatures, wherein said step of certifying comprises the step of said certification server determining, in dependence upon said first and second signatures, that the combination of said second user identity and said second user system does not match the combination of said first user identity and said first user system, further comprising the steps of:

developing a second component signature of each respective component in said second group as present in said second user system at said second time; and

said certification server comparing said second component signatures with said first component signatures to determine whether said first and second user systems satisfy predetermined drift criteria.

14. A method according to claim 13, wherein said step of comparing comprises the step of determining whether a count of the number of said second component signatures which differ from corresponding first component signatures exceeds a predetermined maximum drift number greater than zero.

15. A method according to claim 13, wherein said step of certifying further comprises the step of determining whether said second user identity code is equal to said first user identity code.

16. A digital certification method, comprising the steps of:

storing, accessibly to a certification server, a first signature of a first user identity on a first user system in dependence upon a first user identity code and in dependence further upon a first group of at least one component as present in said first user system at a first time;

at a second time subsequent to said first time, an inquiring system providing a challenge code to a second user system and said second user system developing a second signature in dependence upon a second user identity code and in dependence further upon a second group of at least one component as present in said second user system at said second time;

providing said challenge code and said second signature to said certification server; and

said certification server developing a certification result in dependence upon said second signature and a combination of said challenge code and said first signature.

17. A method according to claim 16, further comprising the step of communicating said certification result to said inquiring system.

18. A digital certification method, comprising the steps of:

forming, at a first time, a first signature dependent upon a first user identity and a first user system in combination;

providing said first signature to a certification server;

generating, in response to an inquiry from an inquiring system at a second time subsequent to said first time, a second signature dependent upon a second user identity and a second user system in combination; and

providing said second signature for comparison with said first signature.

19. A method according to claim 18, wherein said step of forming a first signature comprises the step of developing said first signature in dependence upon a first user identity code and in dependence further upon a first group of at least one component as present in said first user system at said first time.

20. A method according to claim 19, wherein said step of developing said first signature comprises the step of obtaining said first user identity code in response to user input.

21. A method according to claim 18, wherein said second user system is said first user system.

22. A method according to claim 18, wherein said second signature is further dependent upon said inquiry.

23. A method according to claim 18, wherein said second user system receives a challenge code in conjunction with said inquiry,

and wherein said second signature is further dependent upon said challenge code.

24. A method according to claim 18, wherein said first user system comprises a first group of components,

comprising the steps of:

developing a first component signature of each respective component in said first group as present in said first user system at said first time; and

48

providing said first component signatures to said certification server.

25. A method according to claim 24, wherein said second user system comprises a second group of components, wherein said first signature is different from said first component signatures, and wherein the combination of said second user identity and said second user system does not match the combination of said first user identity and said first user system, further comprising the steps of:

developing a second component signature of each respective component in said second group as present in said second user system at said second time; and

providing said second component signatures for comparison with said first component signatures.

26. A digital certification method, comprising the steps of:

providing a challenge code to a user system in response to a request for authorization for said user system;

receiving a real time signature from said user system after said step of providing a challenge code;

providing said challenge code and said real time signature to a certification server; and

A9

receiving a certification result from said certification server after said step of providing said challenge code and said real time signature to said certification server.

27. A method according to claim 26, wherein said real time signature is dependent upon a first user identity and said user system in combination.

28. A method according to claim 27, wherein said real time signature is further dependent upon said challenge code.

29. A digital certification method, comprising the steps of:

storing accessibly to a certification server, at a first time, a first signature dependent upon a first user identity and a first user system in combination;

receiving, at a second time subsequent to said first time, a second signature dependent upon a second user identity and a second user system in combination; and

certifying, in dependence upon said first and second signatures, whether the combination of said second user identity and said second user system match

the combination of said first user identity and said first user system.

30. A method according to claim 29, wherein said second user system is said first user system.

31. A method according to claim 29, wherein said step of certifying comprises the step of certifying, in dependence upon said first and second signatures, whether the combination of said second user identity and said second user system match the combination of said first user identity and said first user system, and that said second signature was generated at a time different from said first time.

32. A method according to claim 29, further comprising the step of receiving, in conjunction with said step of receiving a second signature, a copy of a challenge code,

wherein said second signature is further dependent upon said challenge code.

33. A method according to claim 32, wherein said step of certifying comprises the step of developing a certification result in dependence upon said first and

second signatures and further in dependence upon said challenge code.

34. A method according to claim 29, wherein said step of certifying further comprises the step of providing a certification result to an inquiring system.

35. A method according to claim 29, wherein said first user system comprises a first group of components, comprising the steps of:

receiving a first component signature of each respective component in said first group as present in said first user system at said first time; and

storing said first component signatures accessibly to said certification server.

36. A method according to claim 35, wherein said second user system comprises a second group of components, wherein said first signature is different from said first component signatures, wherein said step of certifying comprises the step of said certification server determining, in dependence upon said first and second signatures, that the combination of said second user identity and said second user system does not match the combination of said first user identity and

said first user system, further comprising the steps of:

receiving a second component signature of each respective component in said second group as present in said second user system at said second time; and

said certification server comparing said second component signatures with said first component signatures to determine whether said first and second user systems satisfy predetermined drift criteria.

37. A method according to claim 36, wherein said step of comparing comprises the step of determining whether a count of the number of said second component signatures which differ from corresponding first component signatures exceeds a predetermined maximum drift number greater than zero.

38. A method according to claim 36, wherein said step of certifying further comprises the step of determining whether said second user identity code is equal to said first user identity code.